DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON DC 20350-2000

Canc frp: Sep 2021

OPNAVNOTE 3070
Ser DNS/20U101074
29 Sep 2020

OPNAV NOTICE 3070

From: Chief of Naval Operations

Subj: OPNAV CRITICAL INFORMATION AND INDICATORS LIST

Ref: (a) SECNAVINST 3070.2A

Encl: (1) OPNAV Critical Information and Indicators List

1. Purpose. To issue the Office of Chief of Naval Operations (OPNAV) critical information and indicators list as required by reference (a).

2. Definitions

a. Critical Information. Specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

b. Indicator. Data derived from friendly detectable actions and open-source information that adversaries can interpret and piece together to reach conclusions or estimates of critical or classified information concerning friendly intentions, capabilities, or activities.

3. Applicability. This directive applies to all within OPNAV.

4. Action. Publish enclosure (1).

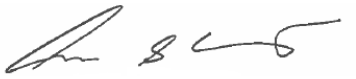
5. Records Management

a. Records created as a result of this notice, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the Department of the Navy Assistant for Administration, Directives and Records Management Division portal page at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx.

b. For questions concerning the management of records related to this notice, change or the records disposition schedules, please contact the local records manager or the OPNAV Records Management Program (DNS-16).

6. Information Management Control. Data collections contained within this notice are exempt from information management control, per Secretary of the Navy Manual 5214.1 of December 2005 part IV, subparagraphs 7f and 7g.

7. Cancellation Contingency. This notice is in effect for 1 year or until it is superseded by another notice, whichever occurs first.



ANDREW S. HAEUPTLE
Director, Navy Staff

Releasability and distribution:
This notice is cleared for public release and is available electronically only via Department of the Navy Issuances Web site, https://www.secnav.navy.mil/doni/default.aspx

OPNAV CRITICAL INFORMATION AND INDICATORS LIST

1. Operations

a. Status or limitations of personnel, equipment, and weapons systems and key contingency concepts processes.

b. Operational command and control structure.

c. Standard operating procedure.

d. Identification, strength, and combat readiness posture of assigned forces.

e. Specific aspects and changes of force protection conditions or information operations conditions.

f. Details and locations of assets used in assigned missions including capabilities, the operational use of the assets, or their state of readiness.

g. Critical ship or activity or regional infrastructure nodes or links.

h. Alert status, response times, and schedules.

i. Exercise, or inspection postures and results.

j. Policies and information regarding rules of engagement, to include the use of weapons and electronic or acoustic warfare systems. Air and ground tactics of U.S., allied, or coalition forces.

k. Mishap or accident information of a privileged nature.

l. Association of daily changing call signs (not international) and authentication procedures with unit designators.

m. Military information support operations.

n. Military deception plans and operations.

o. Special operations forces and unconventional warfare.

p. Special weapons - weapons used in specific procedures or included in special security controls (e.g. nuclear weapons or special access programs).

(1) Specific characteristics and capabilities of weapons.

(2) Doctrine for using various weapons.

(3) Indicators unconventional weapons will be employed.

(4) New weapons that are available or are being employed.

(5) Vulnerabilities and limitations in friendly weapons and weapons systems.

(6) Training related to special weapons and related systems.

(7) Details of transport including routes, schedules, security precautions, call signs, vehicles, and local support.

q. Results of adversary operations or battle damage against U.S. forces that could provide measures of effectiveness to the enemy.

r. Reporting requirements for significant ship or aircraft interaction with foreign military units (e.g., incidents at sea or code for unplanned encounters at sea).

s. Security classification guides.

t. Pre-decisional policy information and proposals.

2. Plans

a. Changes in wartime mission or tasking.

b. Specific information of schedule of forces, equipment, or staging locations.

c. Security classification of a classified operation, program, or project.

d. Intent to mobilize before public announcement.

e. Infrastructure reports.

f. Evacuation routes, procedures, and rally points.

g. Intended operational changes before public announcement.

h. Emergency action plan for heavy and severe weather.

i. Pre-decisional policy information and proposals.

3. Communications and Infrastructure

a. Capabilities, configuration, security measures, limitations, status, upgrades, or proposed changes related to communication systems, to include networks, transmission systems, relay stations, and associated equipment.

b. Technical system architectures, capabilities, vulnerability information, and security assessment reports related to command and control systems or national security systems.

c. Security, network architecture, topology, infrastructure, infrastructure design, and security risk assessment results of Department of the Navy information technology.

d. Location, schematics, capabilities, protection measures, vulnerabilities, and degradation of critical infrastructure.

e. Network architecture diagrams or documents.

f. Information revealing a communications security weakness or physical security weaknesses.

g. Computer passwords, user identifications, or network access paths.

h. Security authorization documentation including data provided to support authorization to operate or connect decisions.

i. Data collected in order to grant access to Department of the Navy information technology, e.g., System Authorization Access Request forms.

j. Pre-decisional policy information and proposals.

4. Intelligence

a. Intelligence sources or methods of gaining intelligence; analytical methods and processes.

b. Intelligence assessments, maps, and locations of intelligence targets.

c. Intelligence, surveillance, and reconnaissance resources.

d. Counterintelligence capabilities.

e. Intelligence gaps and limitations.

f. Security classification guides.

g. Pre-decisional policy information and proposals.

5. Logistics

a. Aggregation of logistics and supply chain data within commercial and government systems.

b. Logistical posture of United States, partner, and allied forces.

c. Port, airfield, and rail operations.

d. Logistics system changes, passwords, and user identifications.

e. Logistics and maintenance capabilities, constraints, shortfalls, and requirements.

f. Consolidated ship maintenance plans.

g. Port visit coordination.

h Logistics Requests.

i. Host-tenant and inter-Service logistics support agreements.

j. Status of supplies.

k. Details about procurements of equipment, parts, and supplies.

l. Transportation of fuel and munitions.

m. Transportation plans.

n. Spares fill rates and levels.

o. Prepositioning of equipment, parts, and supplies.

p. Establishment of logistics bases.

q. Logistics budget or financial documentation.

r. Shipping requests or announcements.

s. Supply and equipment orders or deliveries.

t. New equipment capabilities or limitations.

u. Pre-decisional policy information and proposals.

6. Research, Development, Test, and Engineering and Critical Program Information

a. Weapons systems development schedules (dates, times, locations).

b. Emerging technologies applicable to new weapons systems.

c. Computer software used in weapons systems development, testing, and evaluation.

d. Specific contract criteria stated in a classified contract.

e. Identification of special access elements within a contract or program.

f. Specific program protection plan implementation methods.

g. Status, limitations, or development of weapons systems and design concepts, or processes.

h. Mishap or accident information of a test and evaluation exercise on emerging technologies.

i. Standard operating procedures and other information related to test plans.

j. Intended areas where research, development, test, and engineering experimentation and testing will be conducted.

k. Identification of strength, weakness, and combat readiness of emerging technologies. Test and field experiment results.

l. Test locations, schedules, signatures.

m. Critical program information.

n. Security classification guides.

o. Pre-decisional policy information and proposals.

7. Budget

a. Emergency requisition of funds (or unexpected loss of funding) disclosing details of daily, contingency, or wartime operations.

b. Pre-decisional policy information and proposals.

8. Internet Based Media

a. Personal identifying information.

b. Blank authorization agreement (outlining definitive needs, gaps, limitations, and shortfalls).

c. Full organizational rosters and telephone directories.

d. Contingency plans and continuity of operations.

e. Architectural or floor plans, and diagrams of an organizations building, property, or installation.

f. Pictures containing any security features, e.g., guard shack, barriers, uniformed guards, access badges, safes, locking mechanisms, weapons other than rank, rate, first name, last name, job title, and unit.

g. Pre-decisional policy information and proposals.

9. Personnel

a. Personnel privacy issues and identifiers.

b. Identification and relation of command personnel with security badge, security clearances or access, and special projects.

c. Immunization, medical requirements, health status, and deficiencies.

d. Location, itineraries, and travel modes of key military and civilian personnel.

e. Manpower gains or losses associated with contingency operations or exercise.

f. Training deficiencies impairing mission accomplishment.

g. Lists of personnel in the Department of the Navy cybersecurity workforce, e.g., Department of Defense (DoD) Directive 8140.01 Cyberspace Workforce Management (formerly known as DoD Directive 8570 Information Assurance Training, Certification, and Workforce Management) compliant.

h. Lists of critical or executive personnel with mobile devices.

i. Pre-decisional policy information and proposals.